Office of the Attorney General
Paul G. Summers

Department of Commerce and Insurance
Commissioner Paula Flowers

CONSUMER ALERT

Office of the Attorney General
P.O. Box 20207 Nashville, TN 37202-0207

Department of Commerce and Insurance
Division of Consumer Affairs
500 James Robertson Parkway Nashville, TN 37243

FOR IMMEDIATE RELEASE
Feb. 7, 2006
#06-07

CONTACT:
Sharon Curtis-Flair
(615) 741-5860

ATTORNEY GENERAL WARNS CONSUMERS ABOUT "PHISHING" E-MAIL SCAM REGARDING IRS TAX REFUNDS

Tennessee Attorney General Paul G. Summers warns consumers of an e-mail scam currently occurring in Tennessee in which con artists send e-mails to consumers pretending to be from the Internal Revenue Service (IRS) to obtain your personal information.

Known as "phishing," this high tech scam uses deceptive e-mails to deceive consumers into disclosing information such as bank account information, credit card numbers, Social Security numbers, and other sensitive information. A bogus e-mail recently received by Tennessee consumers claims to come from "support@irs.gov" with the subject heading of "Refund notice." This fraudulent e-mail tells the recipients that they can check on their tax refund by accessing a link to a website address in the e-mail and providing their full names, Social Security numbers (or Taxpayer Identification Numbers), and credit card information to complete the transaction.

"The IRS does not ask for personal identification or financial information via unsolicited e-mails," Attorney General Summers said. "Tennesseans need to know IRS official contact with consumers usually includes a letter on IRS stationary in an IRS envelope."

If you received an unsolicited e-mail purporting to be from the IRS, please take the following steps:

*Do not open any attachments to the e-mail, as they may contain a virus that could infect your computer.
*Contact the IRS at 1-800-829-1040 to verify the taxpayer's account status and determine whether the IRS is trying to contact you about a tax refund.

More information regarding bogus IRS e-mails and identity theft may be found by accessing the IRS website at http://www.irs.gov/newsroom and clicking on "Scams/Consumer Alerts."

This fraudulent IRS e-mail is typical of messages sent to consumers from scammers purporting to be banks or other financial institutions, and consumers are warned not to access the link or provide their personal information. Many phishing e-mails contain a legitimate company's images or logos to help make them appear authentic. Consumers should be wary of e-mails with a sense of urgency, that contain misspelled words or grammatical errors, while asking for personal identification and/or financial information. Also, being able to click anywhere in the e-mail and not just on the link may indicate phishing.

If you receive an e-mail that you believe may be phishing, go to the company website by typing the company's web address into the browser or by doing an Internet search for the company. It is important to not click on the link provided in the e-mail, as it may direct you to a "spoof" website made to look like the legitimate site. Check for fraud alerts posted by the company. Also, report the e-mail to the company. Instructions for making these reports can often be found on the company's Website. If you have provided personal information in response to an e-mail that you believe may have been phishing, alert your bank and the three major credit bureaus. You can report fraud to Equifax at 1-800-525-6285, to Experian at 1-888-EXPERIAN and to TransUnion at 1-800-680-7289. You can also report the suspicious e-mail to the Federal Trade Commission at www.consumer.gov/idtheft or 1-877-IDTHEFT. Finally, contact the Tennessee Division of Consumer Affairs at (615) 741-4737 or www.state.tn.us/consumer.